IN THE CLAIMS

1. (Currently Amended) A data processing apparatus for processing content data provided by a recording or communication medium, said apparatus comprising:

a cryptography process section for executing a cryptography process on said content data; and

a control section for executing control for said cryptography process section, wherein said cryptography process section is configured to:

split a first portion of header data of the content data having data on usage policy into a plurality of first messages,

~~generates~~ generate a first integrity check value or values ~~as~~ to verify integrity of the header data ~~check values for a message~~ by using said plurality of first messages ~~including a usage policy obtained by a header of said content data~~,

~~collates~~ collate said first integrity check value or values to verify said ~~message~~ first portion of the header data,

split a second portion of the header data of the content data having a content key into a plurality of second messages,

generate a ~~generates~~ second integrity check value or values ~~as~~ to verify integrity of the header data by using said plurality of second messages ~~check values for information including at least a content key obtained by said header of said content data~~,

collate ~~collates~~ said second integrity check value or values to verify said second portion of the header data ~~information~~,

generate ~~generates~~ an intermediate integrity check value based on said first integrity check value or values and said second integrity check value or values, and

use ~~uses~~ said intermediate integrity check value to verify said content data corresponding to said first and second integrity check values.

2-3 (canceled).

4. (previously presented) The data processing apparatus according to Claim 1, wherein:

said cryptography process is a DES cryptography process, and

said cryptography process section is configured to execute said DES cryptography process.

5. (currently amended) The data processing apparatus according to Claim 1, wherein:

said first integrity check value or values and said second integrity check value or values are message authentication codes generated in a DES-CBC mode using said message and said information to be checked;

said intermediate integrity check value is a message authentication code generated in said DES-CBC mode using said first integrity check value or values and said second integrity check value or values to be checked, and

said cryptography process section is configured to execute said cryptography process in said DES-CBS mode.

6. (previously presented) The data processing apparatus according to Claim 5, wherein Triple DES is applied in part of a message string to be processed in said DES-CBC mode.

7. (previously presented) The data processing apparatus according to Claim 1, further comprising:

a signature key wherein: said cryptography process section is configured to apply a value generated from said intermediate integrity check value by means of said signature key as a collation value for data verification.

8. (previously presented) The data processing apparatus according to Claim 7, wherein:

said signature key includes a plurality of different signature keys; and

said cryptography process section is configured to apply one of said plurality of different signature keys, which is selected depending on a localization of said content data, to said cryptography process for said intermediate integrity check value to obtain said collation value for data verification.

9. (previously presented) The data processing apparatus according to Claim 8, further comprising:

a common signature key common to all entities of a system for executing a data verifying process; and

an apparatus-specific signature key specific to each apparatus that executes said data verifying process.

10-11 (canceled).

12. (previously presented) The data processing apparatus according to Claim 1, further comprising a recording device for storing data validated by said cryptography process section.

13. (currently amended) The data processing apparatus according to Claim 12, wherein:

said control section suspends storing of said data in said recording device if a process of collating said first integrity check value or values and said second integrity check value or values is not established in said cryptography process executed by said cryptography process section.

14. (previously presented) The data processing apparatus according to Claim 1, further comprising a reproduction process section for reproducing data validated by said cryptography process section.

15. (currently amended) The data processing apparatus according to Claim 14, wherein:

said control section suspends reproducing of said data in said reproduction process section if a process of collating said first integrity check value or values and said second integrity check value or values is not established in said cryptography process executed by said cryptography process section.

16. (currently amended) The data processing apparatus according to Claim 14, further comprising:

control means for collating only header section integrity check values in said data during said cryptography process executed by said cryptography process section to collate said first integrity check value or values and said second integrity check value or values; and

transmitting to said reproduction process section said data for which collation of said header section integrity check values has been established.

17-18 (canceled).

19. (currently amended) A data processing method for processing content data provided by a recording or communication medium, said method comprising:

splitting a first portion of header data of the content data having data on usage policy into a plurality of first messages;

generating first integrity check value or values ~~as~~ to verify integrity of the header data by using said plurality of first messages ~~check values for a message including a usage policy obtained by a header of said content data~~;

collating said first integrity check value or values to verify ~~said message~~said first portion of the header data;

splitting a second portion of the header data of the content data having a content key into a plurality of second messages;

generating second integrity check value or values ~~as~~ to verify integrity of the header data by using said plurality of second messages ~~check values for information including at least a content key obtained by said header of said content data~~;

collating said second integrity check value or values to verify said second portion of the header data~~information~~;

generating an intermediate integrity check value based on said first integrity check value or values and said second integrity check value or values; and

verifying said content data corresponding to said first and second integrity check values using said intermediate integrity check value.

20-21 (canceled).

22. (previously presented) The data processing method according to Claim 19, wherein said cryptography process is a DES cryptography process.

23. (currently amended) The data processing method according to Claim 19, wherein:

said first integrity check value or values and said second integrity check value or values include message authentication codes generated in a DES-CBC mode using said message and said information; and

said intermediate integrity check value is a message authentication code generated in said DES-CBC mode using said first integrity check value or values and said second integrity check value or values.

24. (previously presented) The data processing method according to Claim 19, wherein a value generated from said intermediate integrity check value by means of a signature key-applied cryptography process is applied as a collation value for data verification.

25. (previously presented) The data processing method according to Claim 24, wherein different signature keys are applied to said cryptography process for said intermediate integrity check value depending on a localization of content data, said different signature keys being applied to obtain said collation value for data verification.

26. (previously presented) The data processing method according to Claim 25, further comprising:

selecting and using one of

a common signature key common to all entities of a system for executing a data verifying process; and

an apparatus-specific signature key specific to each apparatus that executes said data verifying process,

said selecting step being based on the localization of said content data.

27-28 (canceled).

29. (previously presented) The data processing method according to Claim 19, further comprising storing validated data after verifying said content data.

30. (currently amended) The data processing method according to Claim 29, further comprising suspending said storing of said validated data if collating of said first integrity check value or values and collating of said second integrity check value or values is not established.

31. (previously presented) The data processing method according to Claim 19, further comprising reproducing data after verifying said content data.

32. (currently amended) The data processing method according to Claim 31, further comprising:

suspending said reproducing of said data if collating of said first integrity check value or values and collating of said second integrity check value or values is not established.

33. (currently amended) The data processing method according to Claim 31,wherein:

said collating of said first integrity check value or values only collates header section integrity check values and transmits said data for which collation of said header section

integrity check values has been established to a reproduction process section for reproduction.

34-35 (canceled).

36. (currently amended) A data verifying value imparting method for a data verifying process, said method comprising:

splitting a first portion of header data of data having data on usage policy into a plurality of first messages;

imparting first integrity check value or values by using said plurality of first messages ~~as integrity check values for a message including a usage policy obtained by a header of content data~~;

splitting a second portion of the header data of the data having a content key into a plurality of second messages;

imparting second integrity check value or values by using said plurality of second messages ~~as integrity check values for information including at least a content key obtained by said header of said content data~~; and

imparting an intermediate integrity check value to data to be verified, said intermediate integrity check value being used to verify content data corresponding to said first integrity check value or values and said second integrity check value or values.

37-38 (canceled).

39. (previously presented) The data verifying value imparting method according to Claim 36 wherein said cryptography process is a DES cryptography process.

40. (currently amended) The data verifying value imparting method according to Claim 36, wherein:

said first integrity check value or values and said second integrity check value or values are message authentication codes generated in a DES-CBC mode using said message and said information; and

said intermediate integrity check value is said message authentication code generated in said DES-CBC mode using said first integrity check value or values and said second integrity check value or values.

41. (previously presented) The data verifying value imparting method according to Claim 36 wherein a value generated from said intermediate integrity check value by means of a signature key-applied cryptography process is applied as a collation value for data verification.

42. (previously presented) The data verifying value imparting method according to Claim 41, wherein different signature keys are applied to said cryptography process for said intermediate integrity check value to obtain said collation value, said different signature keys being applied depending on a localization of content data.

43. (previously presented) The data verifying value imparting method according to claim 42, further comprising:

selecting either a common signature key or an apparatus-specific signature key as one of said different signature keys depending upon the localization of said content data, said common signature key being common to all entities of a system for executing said data verifying process, and said apparatus-specific signature key being specific to each apparatus that executes said data verifying process.

44-45 (canceled).

46. (currently amended) A recording medium recorded with a computer program for executing a data verifying process having certain actions, said actions comprising:

splitting a first portion of header data of data having data on usage policy into a plurality of first messages;

executing a collation process using first integrity check value or values generated by using said plurality of first messages~~as integrity check values for a message including a usage policy obtained by a header of content data~~;

splitting a second portion of the header data of the data having a data key into a plurality of second messages;

executing a collation process using second integrity check value or values generated by using the plurality of second messages~~as integrity check values for information including at least a content key obtained by said header of said content data~~; and

using an intermediate integrity check value to verify said content data corresponding to said first and second integrity check values, said intermediate integrity check value being based on an integrity check value set obtained by combining at least some of said first and second integrity check values together.

47-178 (canceled).

179. (new). The data processing apparatus according to claim 1, wherein the plurality of messages provide multiple input data for a staged encryption.

180. (new). The data processing apparatus according to claim 1, wherein the first and second integrity check values are added to the header of the content data.

181. (new). The data processing method according to claim 19, wherein the plurality of messages provide multiple input data for a staged encryption.

182. (new). The data processing method according to claim 19, wherein the first and second integrity check values are added to the header of the content data.